1 Exercices

Exercice 1.1 Soit $(P_n)_n$ une suite de polynomes telles que

$$\forall n \geqslant 2, \quad P_n(X) = (2-X)P_{n-1}(X) - P_{n-2}(X) \text{ avec } P_0(X) = 1 \text{ et } P_1(X) = 1 - X$$

Donner la décomposition en irréductibles sur $\mathbb{R}$ de P_n.

Exercice 1.2 On note $\alpha = \dfrac{1 + i\sqrt{7}}{2}$.

1. Trouver un polynôme P non nul à coefficients entiers de degré minimal tel que $P(\alpha) = 0$.
2. Montrer que $\mathcal{A} = \{a + b\alpha; \quad (a,b) \in \mathbb{Z}^2\}$ est un anneau.
3. Vérifier que $z \in \mathcal{A}$ implique que $|z|^2 \in \mathbb{N}$.
4. En déduire les éléments inversibles dans $\mathcal{A}$.
5. Parmi les nombres premiers 2, 3, 7, 11, déterminer ceux qui sont irréductibles dans $\mathcal{A}$.

Exercice 1.3

1. Soit $f \in \mathbb{R}[X]$ tel que $\forall x \in \mathbb{R}$, $f(x) \geqslant 0$.
   (a) On suppose que f n'a pas de racine réelle. Montrer qu'il existe $a, b \in \mathbb{R}[X]$ tels que $f = a^2 + b^2$.
   (b) On suppose que f est scindé sur $\mathbb{R}$. Montrer qu'il existe $c \in \mathbb{R}[X]$ tel que $f = c^2$.
   (c) En conclure que f peut toujours s'écrire sous la forme $f = a^2 + b^2$, $a, b \in \mathbb{R}[X]$.
2. Que dire de $f \in \mathbb{R}[X]$ si l'on demande seulement que $\forall x \in \mathbb{R}_+, \quad f(x) \geqslant 0$.

2 Indications

Indication pour l'exercice 1.1 : Pour $x \in \mathbb{R}$ fixé, on obtient une suite récurrente linéaire d'ordre 2. Son polynôme caractéristique admet deux racines réelles si $x \geqslant 4$ donc on obtient la formule explicite de $P_n(x)$ sous la forme d'une expression en radicaux (l'utilisation du binôme permet de se convaincre de l'expression est en fait polynômiale). On obtient ainsi l'expression de $x \mapsto P_n(x)$ sur $[4, +\infty[$ donc sur $\mathbb{R}$ (par unicité du polynôme représentant une fonction polynôme).
Pour les racines, les rechercher sous la forme $x = 2 + 2\cos t$ et utiliser l'expression avec radicaux (on justifiera que l'on peut l'utiliser)

Indication pour l'exercice 1.2 :

1. Elever $\alpha - \dfrac{1}{2}$ au carré et obtenir au final un polynôme unitaire. Si un autre polynôme de degré moindre (donc de degré $\leqslant 1$) annule α alors α est rationnel.
2. Montrer que c'est un sous anneau de $\mathbb{C}$ (pour le produit, utiliser le fait que α^2 est une expression en α, question 1)
3. Il suffit de calculer $|z|^2$!
4. Si z est inversible, justifier que $|z|^2 = 1$ ($uv = 1$ puis passer au module et se rappeler que $|z|^2$ est un entier positif). En déduire que $a^2 + 2b^2 - 1 = -ab$ et majorer $|ab|$ par $\dfrac{1}{2}(a^2 + b^2)$.
5. Si n est non irréductible alors $n = uv$ et passer au module carré. En déduire que dans certains cas, u ou v sont de module 1 donc inversible donc n est irréductible. Dans les cas restants, aboutir à une équation diophantienne, fixé l'une des variables et voir à quelle condition l'autre variable peut être réelle, ce qui élimine d'entrée pas mal de possibilités. Avec les solutions obtenues essayer d'obtenir des décompositions de p.

Indication pour l'exercice 1.3 :

1. Soit $f \in \mathbb{R}[X]$ tel que $\forall x \in \mathbb{R}$, $f(x) \geqslant 0$.
   (a) Tout polynôme sur $\mathbb{R}$ est produit de facteurs linéaires et de trinômes sans racines. Justifier ensuite de tout trinôme sans racines est somme de deux carrés (faire un début de carré) puis utiliser que
   $$(a^2 + b^2)(c^2 + d^2) = |a + ib|^2 \, |c + id|^2$$
   pour voir que le produit de deux sommes de deux carrés est somme de deux carrés.
   (b) Tout polynôme sur $\mathbb{R}$ est produit de facteurs linéaires et de trinômes sans racines. Discuter alors la multiplicité des racines (on pourra s'entrainer avec $\deg f = 2$ puis $\deg f = 4$ dans le doute)
   (c) Tout polynôme sur $\mathbb{R}$ est produit de facteurs linéaires et de trinômes sans racines (je deviens gateux :=))
2. Montrer que l'on peut se ramener au cas où f est scindé sur $\mathbb{R}$ (Tout polynôme sur $\mathbb{R}$ est produit de facteurs linéaires et de trinômes sans racines, le vieux radote :=)). Justifier alors que les racines positives ont une multiplicité paire et se ramener à traiter le cas d'un polynôme scindé sur $\mathbb{R}$ dont les racines sont négatives. Montrer alors que f s'écrit $P + xQ$ où P et Q sont positifs sur $\mathbb{R}$.

3 Corrections

Correction de l'exercice 1.1 : Une récurrence double montre que $\forall n \in \mathbb{N}$, $\deg P_n = n$ (poser $(\mathcal{P}_n)$: $\deg P_n = n$ et $\deg P_{n+1} = n+1$. Pour l'hérédité, $(2-X)P_n$ est de degré $n+1$ et P_{n-1} est de degré n donc $P_{n+1} = (2-X)P_n - P_{n-1}(X)$ est degré $n+1$).
Si a_n désigne le coefficient dominant de P_n, le fait que $\deg P_n = n$ et la relation de récurrence satisfaite par les P_n montre que $\forall n \geqslant 1, \quad a_{n+1} = -a_n$ donc $a_n = (-1)^{n-1}a_1 = (-1)^n$.
Pour factoriser P_n, nous allons rechercher ses racines complexes, ce qui nécessite à priori l'explicitation de P_n.

- **Explicitation de** $P_n(x)$ lorsque $x \in]4, +\infty[$.
  Pour cela, nous allons travailler à x fixé dans $\mathbb{R}$. Le polynôme caractéristique de cette relation de récurrence est

$$T^2 = (2-x)T - 1$$

dont le discriminant est $\Delta = (2-x)^2 - 4 = x^2 - 4x = x(x-4)$. Pour que ce discriminant soit strictement positif, nous exigeons que $x \in]4, +\infty[$. Dans ce cas, les racines sont $T_\pm(x) = \dfrac{2-x \pm \sqrt{x(x-4)}}{2}$ et donc il existe deux constantes (par rapport à n) réelles $\alpha(x)$ et $\beta(x)$ tels que

$$\begin{array}{rcl} \forall x & \in &]4, +\infty[, \quad \forall n \geqslant 2, \\ P_n(x) & = & \alpha(x)\left(\dfrac{2-x+\sqrt{x(x-4)}}{2}\right)^n + \beta(x)\left(\dfrac{2-x-\sqrt{x(x-4)}}{2}\right)^n. \end{array}$$

Explicitons $\alpha(x)$ et $\beta(x)$. En particularisant la formule précédente pour $n = 0$ et 1, on obtient

$$\left\{ \begin{array}{c} \alpha(x) + \beta(x) = 1 \\ \alpha(x)\dfrac{2-x+\sqrt{x(x-4)}}{2} + \beta(x)\dfrac{2-x-\sqrt{x(x-4)}}{2} = 1-x \end{array} \right.$$

et une résolution directe par substitution nous montre que

$$\left\{ \begin{array}{l} \alpha(x) = \dfrac{-x+\sqrt{x(x-4)}}{2\sqrt{x(x-4)}} \\ \beta(x) = \dfrac{x+\sqrt{x(x-4)}}{2\sqrt{x(x-4)}} \end{array} \right.$$

ce qui nous donne au final

$$\begin{array}{rcl} \forall x & \in &]4, +\infty[, \quad \forall n \geqslant 2 : \\ P_n(x) & = & \dfrac{-x+\sqrt{x(x-4)}}{2\sqrt{x(x-4)}}\left(\dfrac{2-x+\sqrt{x(x-4)}}{2}\right)^n + \dfrac{x+\sqrt{x(x-4)}}{2\sqrt{x(x-4)}}\left(\dfrac{2-x-\sqrt{x(x-4)}}{2}\right)^n \end{array}$$

Remarque : Cette formule semble être un peu barbare mais si, par analogie avec les complexes et $i = \sqrt{-1}$, on admet que le conjugué de $P+\sqrt{Q}$ est $P-\sqrt{Q}$ alors $P_n(X)$ n'est que la "partie imaginaire" de $\dfrac{(-X+\sqrt{X(X-4)})(2-X+\sqrt{X(X-4)})^n}{2^n}$ *donc il s'agit d'un polynôme*

- **Explicitation du polynôme** P_n.
  Contre toute attente, l'expression

$$\frac{-x+\sqrt{x(x-4)}}{2\sqrt{x(x-4)}}\left(\frac{2-x+\sqrt{x(x-4)}}{2}\right)^n + \frac{x+\sqrt{x(x-4)}}{2\sqrt{x(x-4)}}\left(\frac{2-x-\sqrt{x(x-4)}}{2}\right)^n$$

est un polynôme de $\mathbb{R}[X]$. En effet, la formule du binôme de Newton montre que

$$\begin{array}{rcl} \left(2-x+\sqrt{x(x-4)}\right)^n & = & \left(\sqrt{x(x-4)}+2-x\right)^n = \displaystyle\sum_{k=0}^{n}\binom{n}{k}\left(\sqrt{x(x-4)}\right)^k(2-x)^{n-k} \\ \left(2-x-\sqrt{x(x-4)}\right)^n & = & \left(-\sqrt{x(x-4)}+2-x\right)^n = \displaystyle\sum_{k=0}^{n}\binom{n}{k}\left(-\sqrt{x(x-4)}\right)^k(2-x)^{n-k} \\ & = & \displaystyle\sum_{k=0}^{n}\binom{n}{k}(-1)^k\left(\sqrt{x(x-4)}\right)^k(2-x)^{n-k}, \end{array}$$

ce qui nous fournit

$$\begin{aligned}\left(2-x-\sqrt{x(x-4)}\right)^n-\left(2-x+\sqrt{x(x-4)}\right)^n &= \sum_{k=0}^{n}\binom{n}{k}((-1)^k-1)\left(\sqrt{x(x-4)}\right)^k(2-x)^{n-k}\\ &= -2\sum_{0\leqslant 2k+1\leqslant n}\binom{n}{2k+1}\left(\sqrt{x(x-4)}\right)^{2k+1}(2-x)^{n-(2k+1)}\\ &= -2\sqrt{x(x-4)}\sum_{0\leqslant 2k+1\leqslant n}\binom{n}{2k+1}(x(x-4))^k(2-x)^{n-(2k+1)} \quad (1)\end{aligned}$$

et

$$\begin{aligned}\left(2-x-\sqrt{x(x-4)}\right)^n+\left(2-x+\sqrt{x(x-4)}\right)^n &= \sum_{k=0}^{n}\binom{n}{k}(1+(-1)^k)\left(\sqrt{x(x-4)}\right)^k(2-x)^{n-k}\\ &= 2\sum_{0\leqslant 2k\leqslant n}\binom{n}{2k}\left(\sqrt{x(x-4)}\right)^{2k}(2-x)^{n-2k}\\ &= 2\sum_{0\leqslant 2k\leqslant n}\binom{n}{2k}(x(x-4))^k(2-x)^{n-2k)} \quad (2)\end{aligned}$$

L'expression de P_n sous forme de radicaux (valable si $x\in]4,+\infty[$) nous permet d'écrire

$$\begin{aligned}2^{n+1}\sqrt{x(x-4)}P_n(x) &= \left(-x+\sqrt{x(x-4)}\right)\left(2-x+\sqrt{x(x-4)}\right)^n+\left(x+\sqrt{x(x-4)}\right)\left(2-x-\sqrt{x(x-4)}\right)^n\\ &= x\left[\left(2-x-\sqrt{x(x-4)}\right)^n-\left(2-x+\sqrt{x(x-4)}\right)^n\right]\\ &\quad +\sqrt{x(x-4)}\left[\left(2-x+\sqrt{x(x-4)}\right)^n+\left(2-x-\sqrt{x(x-4)}\right)^n\right],\end{aligned}$$

ce qui combiné aux égalités (1) et (2) nous donne

$$\begin{aligned}2^{n+1}\sqrt{x(x-4)}P_n(x) &= -2x\sqrt{x(x-4)}\sum_{0\leqslant 2k+1\leqslant n}\binom{n}{2k+1}(x(x-4))^k(2-x)^{n-(2k+1)}\\ &\quad +\sqrt{x(x-4)}2\sum_{0\leqslant 2k\leqslant n}\binom{n}{2k}(x(x-4))^k(2-x)^{n-2k)}\end{aligned}$$

donc on en déduit que

$$P_n(x)=\frac{1}{2^n}\left[-x\sum_{0\leqslant 2k+1\leqslant n}\binom{n}{2k+1}(x(x-4))^k(2-x)^{n-(2k+1)}+\sum_{0\leqslant 2k\leqslant n}\binom{n}{2k}(x(x-4))^k(2-x)^{n-2k)}\right],$$

ce qui montre que l'expression obtenue est bien polynômiale. En outre, puisque les polynômes P_n et

$$\frac{1}{2^n}\left[-X\sum_{0\leqslant 2k+1\leqslant n}\binom{n}{2k+1}(X(X-4))^k(2-X)^{n-(2k+1)}+\sum_{0\leqslant 2k\leqslant n}\binom{n}{2k}(X(X-4))^k(2-X)^{n-2k)}\right]$$

coïncident sur l'ensemble infini $]4,+\infty[$, on en déduit qu'ils sont égaux. Par conséquent,

$$\forall n\in\mathbb{N},\quad P_n(X)=\frac{1}{2^n}\left[-X\sum_{0\leqslant 2k+1\leqslant n}\binom{n}{2k+1}(X(X-4))^k(2-X)^{n-(2k+1)}+\sum_{0\leqslant 2k\leqslant n}\binom{n}{2k}(X(X-4))^k(2-X)^{n-2k)}\right]$$

- **Détermination des racines de P_n.**
Il ne reste plus qu'à déterminer les racines d'un tel polynôme ! Pour cela, on recherche à priori la forme des racines et l'analogie formelle située dans la remarque de **la détermination de P_n lorsque** $x\in]4,+\infty[$ va nous aider.
Recherche formelle
On remarque pour commencer que

$$X(X-4)=X^2-4X=(X-2)^2-4=4\left[\left(\frac{X}{2}-1\right)^2-1\right].$$

On remarque alors que si $\dfrac{X}{2}-1=\cos\varphi \Leftrightarrow X=2-2\cos\varphi$ et l'on a

$$X(X-4)=4\left[\left(\frac{X}{2}-1\right)^2-1\right]=4(-1+\cos^2\varphi)=-4\sin^2\varphi=(2i\sin\varphi)^2$$

Avec un tel choix de $X=2-2\cos\varphi$ on a $\sqrt{X(X-4)}=2i\sin\varphi$ et son conjugée complexe est $-2i\sin\varphi=-\sqrt{X(X-4)}$.
Déterminons les racines de P_n de la forme $2-2\cos\varphi$
Par périodicité et parité de la fonction cos, on peut supposer que $\boxed{\varphi\in[0,\pi]}$. Nous utilisons alors le raisonnement de la partie **détermination de $P_n(x)$ lorsque $x\in]4,+\infty[$**. Puisque $(P_n(2-2\cos\varphi))_{n\geqslant 0}$ est une suite récurrente linéaire d'ordre 2 dont le polynôme caractéristique est

$$T^2=(2-(2-2\cos\varphi))T-1\Leftrightarrow T^2=2T\cos\varphi-1\Leftrightarrow T^2-2T\cos\varphi+1=0$$

dont les racines sont

$$T_\pm=\cos\varphi\pm i\sin\varphi=e^{\pm i\varphi}.$$

Si l'on suppose que

$$e^{i\varphi}\neq e^{-i\varphi}\Leftrightarrow\varphi\neq-\varphi\bmod 2\pi\Leftrightarrow 2\varphi\neq 0\bmod 2\pi\Leftrightarrow\varphi\neq 0\bmod\pi\Leftrightarrow\varphi\in]0,\pi[$$

ce polynôme admet deux racines complexes distinctes donc ils existent deux complexes $\alpha(\varphi)$ et $\beta(\varphi)$ tels que

$$\forall n\in\mathbb{N},\quad P_n(2-2\cos\varphi)=\alpha(\varphi)(e^{i\varphi})^n+\beta(\varphi)(e^{-i\varphi})^n=\alpha(\varphi)e^{in\varphi}+\beta(\varphi)e^{-in\varphi}$$

En particularisant la formule précédente pour $n=0$ et 1, on obtient

$$\left\{\begin{array}{rcl}\alpha(\varphi)+\beta(\varphi) & = & 1\\ \alpha(\varphi)e^{i\varphi}+\beta(\varphi)e^{-i\varphi} & = & 1-(2-2\cos\varphi)\quad=2\cos\varphi-1\quad=e^{i\varphi}+e^{-i\varphi}-1\end{array}\right.$$

et une résolution directe nous montre que

$$\left\{\begin{array}{l}\alpha(x)=\dfrac{-1+\exp(i\varphi)}{2i\sin\varphi}\\ \beta(x)=-\dfrac{-1+\exp(-i\varphi)}{2i\sin\varphi}\end{array}\right.,$$

(on remarque que l'hypothèse $\varphi\in]0,\pi[$ est utilisé ici pour effectuer la division) ce qui nous donne

$$P_n(2-2\cos\varphi)=\frac{(-1+e^{i\varphi})e^{in\varphi}-(-1+e^{-i\varphi})e^{-in\varphi}}{2i\sin\varphi}$$

On remarque ensuite que les deux termes de la somme sont conjugués ($z-\overline{z}=2i\,\mathrm{Im}(z)$) donc on peut écrire

$$\begin{array}{rcl}P_n(2-2\cos\varphi) & = & \dfrac{2i\,\mathrm{Im}\left[(-1+e^{i\varphi})e^{in\varphi}\right]}{2i\sin\varphi}=\dfrac{\mathrm{Im}\left[(-1+e^{i\varphi})e^{in\varphi}\right]}{\sin\varphi}=\dfrac{\mathrm{Im}\left[(e^{i\varphi/2}-e^{-i\varphi/2})e^{i(n+1/2)\varphi}\right]}{\sin\varphi}\\ & = & \dfrac{\mathrm{Im}(2i\sin\frac{\varphi}{2}e^{i(n+1/2)\varphi})}{\sin\varphi}=\dfrac{2\sin\frac{\varphi}{2}\cos(n+\frac{1}{2})\varphi}{2\sin\frac{\varphi}{2}\cos\frac{\varphi}{2}}=\dfrac{\cos(n+\frac{1}{2})\varphi}{\cos\frac{\varphi}{2}}\end{array}$$

Puisque l'on a supposer $\varphi\in]0,\pi[$ alors $\dfrac{\varphi}{2}\in]0,\dfrac{\pi}{2}[$ donc $\cos\dfrac{\varphi}{2}\neq 0$ et l'on est assuré que le quotient précédent existe. On obtient alors

$$\begin{array}{rcl}P_n(2-2\cos\varphi) & = & 0\Leftrightarrow\cos(n+\frac{1}{2})\varphi=0\Leftrightarrow(n+\frac{1}{2})\varphi=\frac{\pi}{2}+k\pi=\frac{(2k+1)\pi}{2},\quad k\in\mathbb{Z}\\ & \Leftrightarrow & \varphi=\dfrac{(2k+1)\pi}{2n+1},\quad k\in\mathbb{Z}\end{array}$$

Puisque l'on doit avoir $\varphi\in]0,\pi[$, on en déduit que $k\in[\![0,n-1]\!]$ (en particulier, cela implique que $n\geqslant 1$) La fonction $x\mapsto 2-2\cos x$ étant injective sur $]0,\pi[$ et puisque les réels $\left(\dfrac{(2k+1)\pi}{2n+1}\right)_{k\in[\![0,n-1]\!]}$ appartiennent à $]0,\pi[$, on en déduit que les n réels

$$x_k=2-2\cos\frac{(2k+1)\pi}{2n+1},\quad k\in[\![0,n-1]\!]$$

sont deux à deux distincts.et ce sont des racines de P_n. Or nous savons que P_n est un polynôme de degré n (cf. le début de l'exercice) donc P_n est scindé à racines simples sur $\mathbb{R}$ et ses racines sont les

$$2-2\cos\frac{(2k+1)\pi}{2n+1} =, \quad k\in[\,[0,n-1]\,]$$

Au début de l'exercice, nous avons montrer que le coefficient dominant de P_n est $(-1)^n$ donc la décomposition sur $\mathbb{R}$ de P_n est donnée par :

$$\forall n\geqslant 1,\quad P_n(X)=(-1)^n\prod_{k=0}^{n-1}\left(X-2+2\cos\frac{(2k+1)\pi}{2n+1}\right)$$

Pour finir, on constate que le polynôme $P_0=1$ ne possède pas de racines.

Correction de l'exercice 1.2 :

1. $\alpha=\dfrac{1+i\sqrt{7}}{2}\Leftrightarrow 2\alpha-1=i\sqrt{7}\Leftrightarrow(2\alpha-1)^2=-7\Leftrightarrow 4\alpha^2-4\alpha+8=0\Leftrightarrow\alpha^2-\alpha+2=0.$
Par conséquent, le polynôme $P(X)=X^2-X+2$ convient. S'il existe un polynôme non nul $Q\in\mathbb{Z}[X]$ tel que $\deg Q<\deg P=2$ alors Q est de la forme $Q(X)=aX+b$ avec a,b deux entiers naturels. Puisque Q est non nul et qu'il admet α comme racine alors $a\neq 0$ (un polynôme constant possédant une racine est nul). Par conséquent, on a

$$Q(\alpha)=0\Leftrightarrow a\alpha+b=0\Leftrightarrow\alpha\underset{a\neq0}{=}-\frac{b}{a}\in\mathbb{Q}\Rightarrow\frac{1+i\sqrt{7}}{2}\in\mathbb{Q}\Rightarrow i\sqrt{7}\in\mathbb{Q}$$

ce qui est clairement impossible. Donc $P(X)=X^2-X+2$ est un polynôme non nul de $\mathbb{Z}[X]$ de degré minimal admettant α comme racine.

2. $\mathcal{A}$ étant inclu dans $(\mathbb{C},+,\times)$, il suffit de montrer que $\mathcal{A}$ est un sous-anneau de $\mathbb{C}$, c'est-à-dire qu'il contient l'élément neutre de l'addition (ici 0) , l'élément neutre de la multiplication (ici 1) et qu'il est stable par addition, soustraction et multiplication.

   - $0=0+0\times\alpha\in\mathcal{A}$ et $1=1+0\times\alpha\in\mathcal{A}$
   - Soient z et z' deux éléments de $\mathcal{A}$. Alors il existe a,b,c,d quatre entiers relatifs tels que $z=a+b\alpha$ et $z'=c+d\alpha$. On a alors
   $$z\pm z'=(a+b\alpha)\pm(c+d\alpha)=\underbrace{(a\pm c)}_{\in\mathbb{Z}}+\underbrace{(b\pm d)}_{\in\mathbb{Z}}\alpha\in\mathcal{A}$$
   donc $\mathcal{A}$ est stable par addition et soustraction. En utilisant que $\alpha^2=\alpha-2$ (α est racine de P), on a également
   $$\begin{aligned} z\times z' &= (a+b\alpha)(c+d\alpha)=ac+ad\alpha+bc\alpha+bd\alpha^2=ac+(ad+bc)\alpha+bd(\alpha-2)\\ &= \underbrace{(ac-2bd)}_{\in\mathbb{Z}}+\underbrace{(ad+bc+bd)}_{\in\mathbb{Z}}\alpha\in\mathcal{A}\end{aligned}$$
   donc $\mathcal{A}$ est stable par multiplication, ce qui achève la preuve que $\mathcal{A}$ est un anneau.

3. Si $z\in\mathcal{A}$ alors il existe deux entiers naturels a et b tels que $z=a+b\alpha=a+\dfrac{b}{2}+i\dfrac{b\sqrt{7}}{2}$ et l'on a
$$|z|^2=(a+\frac{b}{2})^2+\frac{7b^2}{4}=a^2+ab+2b^2\in\mathbb{N}$$

4. Si z est inversible alors il existe $z'\in\mathcal{A}$ tel que $zz'=1$. En passant au module carré, on obtient que $|z|^2|z'|^2=1$. Or $|z|^2$ et $|z'|^2$ sont deux entiers naturels positifs et le produit de deux entiers naturels positifs est égal à 1 si et seulement chacun de ces entiers naturels est égal à 1. Autrement, on vient de montrer que $|z|^2=1$, ce qui s'écrit encore $a^2+ab+2b^2=1$ si $z=a+b\alpha$. En utilisant la majoration classique $|ab|\leqslant\dfrac{1}{2}(a^2+b^2)$, on obtient
$$\begin{aligned} a^2+ab+2b^2 &= 1\Leftrightarrow a^2+2b^2-1=-ab\leqslant|ab|\leqslant\frac{1}{2}(a^2+b^2)\Leftrightarrow a^2+2b^2-\frac{1}{2}(a^2+b^2)\leqslant 1\\ &\Leftrightarrow \frac{a^2}{2}+\frac{3b^2}{2}\leqslant 1\Leftrightarrow .a^2+3b^2\leqslant 2.\end{aligned}$$
Si $b\neq0$, puisque b est un entier relatif, on a
$$b^2\geqslant 1\Rightarrow 3b^2\geqslant 3\Rightarrow a^2+3b^2\geqslant 3>2$$

ce qui est impossible. Par conséquent $b=0$ et l'égalité $a^2+ab+2b^2=1$ montre que $a^2=1$ donc $a=\pm 1$. Ainsi, si un élément z de $\mathcal{A}$ est inversible alors $z=\pm 1\in\mathcal{A}$. Réciproquement ± 1 est inversible dans $\mathcal{A}$ car $(\pm 1)(\pm 1)=1$ donc ± 1 est son propre inverse.
Conclusion : les éléments inversibles dans $\mathcal{A}$ sont simplements les deux nombres 1 et -1.

5. *Rappel : un élément non nul x d'un anneau $(A,+,\times)$ est dit irréductible si l'égalité $x=ab$, où a et b sont deux éléments de A, implique a ou b est inversible dans A.*
Par conséquent, un élément non nul x est réductible dans A si l'on peut l'écrire $x=ab$, où a et b sont deux éléments non inversibles de A.
Cas particulier de l'anneau $\mathcal{A}$: Soit p est un nombre premier dans $\mathbb{N}$ (donc $p=p+0\times\alpha$ est un élément de $\mathcal{A}$). Si $p=zz'$, où z et z' sont deux éléments de $\mathcal{A}$, alors en passant au module carré, on obtient $p^2=|z|^2|z'|^2$. Puisque $|z|^2$ et $|z'|^2$ sont des entiers naturels (cf.3) et que leur produit est égal à p^2, l'unicité de la décomposition en facteurs premiers dans $\mathbb{N}$ montre que

$$\begin{cases} |z|^2=p \text{ et } |z'|^2=p \\ \text{ou} \\ |z|^2=1 \text{ et } |z'|^2=p^2 \\ \text{ou} \\ |z|^2=p^2 \text{ et } |z'|^2=1 \end{cases}$$

Si l'on montre que l'égalité $|z|^2=p$ est impossible alors nécessairement $|z|^2=1$ ou $|z'|^2=1$. Dans ce cas, la question 4) montre que z ou z' est inversible dans $\mathcal{A}$ donc p est irréductible dans $\mathcal{A}$.
Si l'égalité $|z|^2=p$ admet des solutions, leurs explicitations nous permettrons de connaitre les valeurs possibles de z (et donc de z').
Si $z=a+b\alpha$, avec $a,b\in\mathbb{Z}$, la question 3) montre que l'égalité $|z|^2=p$ s'écrit encore

$$(E_p)\qquad a^2+ab+2b^2=p$$

Commençons par quelques remarques :
Remarque 1 : b ne peut être nul, sinon $a^2=p$, donc a divise p et p étant premier, on a $a=1$ ou $a=p$, ce qui est impossible car $1^2\neq p$ et $p^2\neq p$.
Remarque 2 : pour b fixé, on peut voir l'équation (E_p) comme une équation du second degré en a. Son discriminant est $\Delta=b^2-4(2b^2-p)=4p-7b^2$. Si cediscriminant est strictement négatif, alors l'équation ne peut avoir de solutions réelles donc entières. Ceci se réalise ssi

$$\Delta<0\Leftrightarrow b^2>\frac{4p}{7}\underset{\sqrt{b^2}=|b|}{\Leftrightarrow}|b|>\sqrt{\frac{4p}{7}}.$$

Par conséquent, l'équation (E_p) ne peut avoir de solutions entières si $|b|>\sqrt{\frac{4p}{7}}$.
En considèrant cette même équation (E_p) pour a fixé, un raisonnement analogue montre que l'équation (E_p) ne peut avoir de solutions entières si $|a|>\sqrt{\frac{8p}{7}}$.
Conclusion : en utilisant les remarques 1 et 2, on obtient que les seules solutions (a,b) possibles à l'équation (E_p) sont celles pour lesquelles

$$|a|\leqslant\sqrt{\frac{8p}{7}}\text{ et }0<|b|\leqslant\sqrt{\frac{4p}{7}}$$

Si $p=2$ alors $0<|b|\leqslant\sqrt{\frac{8}{7}}\simeq 1.07$ donc $b\in\{1,-1\}$. Dans ce cas $b^2=1$ et l'équation (E_2) devient

$$a^2+ab+2=2\Leftrightarrow a^2+ab=0\Leftrightarrow a=0\text{ ou }a=-b$$

Par conséquent, l'équation (E_2) admet pour ensemble de solutions

$$S_2=\{(0,-1),(0,1),(1,-1),(-1,1),\}$$

Si $p=3$ alors $0<|b|\leqslant\sqrt{\frac{12}{7}}\simeq 1.31$ donc $b\in\{1,-1\}$. Dans ce cas, on a de nouveau $b^2=1$ et l'équation (E_3) devient

$$a^2+ab+2=3\Leftrightarrow a^2+ab-1=0\Leftrightarrow a=\frac{-b\pm\sqrt{5}}{2}\notin\mathbb{Z}$$

Par conséquent, l'équation (E_3) n'admet aucune solution et $S_3 = \emptyset$

Si $p = 7$ alors $0 < |b| \leqslant \sqrt{\dfrac{4 \times 7}{7}} = 2$ donc $b \in \{-2, -1, 1, 2\}$.
Supposons que $b \in \{-1, 1\}$ alors $b^2 = 1$ et l'équation (E_7) devient

$$a^2 + ab + 2 = 7 \Leftrightarrow a^2 + ab - 5 = 0 \Leftrightarrow a = \frac{-b \pm \sqrt{26}}{2} \notin \mathbb{Z},$$

ce qui est impossible.
Supposons que $b \in \{-2, 2\}$ alors $b^2 = 4$ et l'équation (E_7) devient

$$a^2 + ab + 8 = 7 \Leftrightarrow a^2 + ab + 1 = 0 \Leftrightarrow a = \frac{-b}{2}$$

Par conséquent, l'équation (E_7) admet pour ensemble de solutions

$$S_7 = \{(1, -2), (-1, 2)\}$$

Si $p = 11$ alors $0 < |b| \leqslant \sqrt{\dfrac{4 \times 11}{7}} \simeq 2.51$ donc $b \in \{-2, -1, 1, 2\}$.
Supposons que $b \in \{-1, 1\}$ alors on a $b^2 = 1$ et l'équation (E_{11}) devient

$$a^2 + ab + 2 = 11 \Leftrightarrow a^2 + ab - 9 = 0 \Leftrightarrow a = \frac{-b \pm \sqrt{37}}{2} \notin \mathbb{Z},$$

ce qui impossible.
Supposons que $b \in \{-2, 2\}$ alors on a $b^2 = 4$ et l'équation (E_{11}) devient

$$a^2 + ab + 8 = 11 \Leftrightarrow a^2 + ab - 3 = 0 \underset{\Delta = b^2 + 12 = 16}{\Leftrightarrow} a = \frac{-b + 4}{2}$$

Par conséquent, l'équation (E_7) admet pour ensemble de solutions

$$S_{11} = \{(3, -2), (1, 2)\}$$

Ainsi, la seule équation impossible est (E_3) ce qui implique d'après les raisonnements du début que 3 est irréductible dans $\mathcal{A}$.
Par contre, les autres équations sont solubles. Rappellons que les solutions (a, b) des équations (E_p) correspondantes aux éventuels éléments z, z' de $\mathcal{A}$ pour lesquels $p = zz'$, $z = a + b\alpha$ et $|z|^2 = p$. En testant les diverses valeurs possibles pour z et z' obtenues grâce aux solutions de (E_p), on obtient que
Pour $p = 2$, en considérant les solutions $(0, -1)$ et $(-1, 1)$ de (E_2), on aboutit aux éléments de $\mathcal{A}$

$$z = -\frac{1 + i\sqrt{7}}{2}, \quad z' = -1 + \frac{1 + i\sqrt{7}}{2} = \frac{-1 + i\sqrt{7}}{2} \text{ et l'on a } zz' = \left(-\frac{1 + i\sqrt{7}}{2}\right)\left(\frac{-1 + i\sqrt{7}}{2}\right) = 2.$$

Puisque $|z|^2 \neq 1$ et $|z'|^2 \neq 1$, aucun des deux complexes z et z' n'est inversible dans $\mathcal{A}$, ce qui montre que 2 n'est pas irréductible dans $\mathcal{A}$
Pour $p = 7$, en considérant les solutions de $(1, -2)$ et $(-1, 2)$ de (E_7), on aboutit aux éléments de $\mathcal{A}$

$$z = 1 - 2 \times \frac{1 + i\sqrt{7}}{2} = i\sqrt{7}, \quad z' = -1 + 2 \times \frac{1 + i\sqrt{7}}{2} = -i\sqrt{7} \text{ et l'on a } zz' = 7$$

Puisque $|z|^2 \neq 1$ et $|z'|^2 \neq 1$, aucun des deux complexes z et z' n'est inversible dans $\mathcal{A}$, ce qui montre que 7 n'est pas irréductible dans $\mathcal{A}$.
Pour $p = 11$, en considérant les solutions $(3, -2)$ et $(1, 2)$ de (E_{11}), on aboutit aux éléments de $\mathcal{A}$

$$z = 3 - 2 \times \frac{1 + i\sqrt{7}}{2} = 2 - i\sqrt{7}, \quad z' = 1 + 2 \times \frac{1 + i\sqrt{7}}{2} = 2 + i\sqrt{7} \text{ et l'on a } zz' = 11$$

Puisque $|z|^2 \neq 1$ et $|z'|^2 \neq 1$, aucun des deux complexes z et z' n'est inversible dans $\mathcal{A}$, ce qui montre que 11 n'est pas irréductible dans $\mathcal{A}$.
Conclusion : seul 3 est irréductible dans $\mathcal{A}$.
Remarque : *on rappelle que deux éléments sont dit associés ssi ils sont égaux à un inversible près. Par conséquent, deux éléments z et z' de $\mathcal{A}$ sont associés ssi $z' = \pm z$.*
Dans l'anneau $\mathcal{A}$, si un élément z est tel que $|z|^2$ est un nombre premier p alors z est irréductible. En effet, si $z = wt$ alors en passant à la norme carré, on a $|w|^2 |t|^2 = p$. Puisque $|w|^2$ et $|t|^2$ sont des entiers naturels et que p est premier, on en déduit que $|w|^2 = 1$ ou $|t|^2 = 1$. Par la caractérisation des inversibles de $\mathcal{A}$ (question 3), on obtient que w ou t sont des inversibles, ce qui montre que z est irréductible.Ainsi,

- *pour $p=2$ et 11, on constate que p est le produit de deux irréductibles z, z'de $\mathcal{A}$ et que z et z' ne sont pas associés.*
- *Pour $p=7$, on constate que p est le produit de deux irréductibles z, z' qui sont associés donc p est associé à z^2, où z est irréductible dans $\mathcal{A}$.*
- *Pour $p=3$, p est irréductible dans $\mathcal{A}$.*

Il existe une explication à ces résultats à priori épars.
Les remarques 1 et 2 montrent que $0<|b|<p$ et puisque p est un nombre premier, cela implique que b est premier à p (si d divise b et p alors $d=1$ ou $d=p$, si $d=p$ alors p divise b donc $b=pk \Rightarrow p\,|k|=|b|<k \Rightarrow p<1$!).
En particulier, la classe $\overline{b}=b \bmod p$ est inversible dans l'anneau $\mathbb{Z}/p\mathbb{Z}$.
Ce fait remarquable, combinée au fait que $p=0 \bmod p$, va nous permettre de ramener l'existence de l'équation (E_p) à l'existence d'une équation polynômiale à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Pour cela, pour tout entier naturel x, on note $\overline{x}$ la classe modulo p.
Soit $(a,-b)$ une solution de (E_p) (on peux toujours remplacer b par $-b$), on a $\overline{a}^2-\overline{a}\overline{b}+2\overline{b}^2=0 \bmod p$. Puisque $\overline{b}$ étant inversible dans $\mathbb{Z}/p\mathbb{Z}$, on peut "diviser" par $\overline{b}^2$ (autrement dit multiplier par $(\overline{b}^{-1})^2$ ce qui nous donne

$$\overline{a}^2-\overline{a}\overline{b}+\overline{2}\overline{b}^2=0 \bmod p \underset{\times(\overline{b}^{-1})^2}{\Leftrightarrow} (\overline{a}\overline{b}^{-1})^2-\overline{a}\overline{b}^{-1}+\overline{2}=0 \bmod p$$

En posant $\overline{x}=\overline{a}\overline{b}^{-1}$, on obtient que $\overline{x}$ est racine du polynôme $R_p(X)=X^2-X+\overline{2}$ à coefficients dans $\mathbb{Z}/p\mathbb{Z}$.
Remarquons que ce polynôme n'est rien d'autre que la réduction modulo p du polynôme minimal de α qui engendre A.
Dresser le tableau des valeurs de R_p selon les valeurs de p

$p=2$	$\overline{x}$	$\overline{0}$	$\overline{1}$
	$R_2(\overline{x})$	$\overline{0}$	$\overline{0}$

$p=3$	$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
	$R_3(\overline{x})$	$\overline{2}$	$\overline{2}$	$\overline{1}$

$p=7$	$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
	$R_7(\overline{x})$	$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{4}$

$p=11$	$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
	$R_{11}(\overline{x})$	$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{3}$	$\overline{0}$	$\overline{10}$	$\overline{0}$	$\overline{3}$	$\overline{8}$	$\overline{4}$

donc nous disposons de la factorisation de R_p en produits d'irréductibles dans $Z/pZ[X]$ donner par

$$R_2(X)=X(X-\overline{1}),\quad R_3(X)=R_3(X),\quad R_7(X)=(X-\overline{4})^2,\quad R_{11}(X)=(X-\overline{5})(X-\overline{7})$$

On constate que lorsque le polynôme R_p (réduction de X^2-X+2 modulo p) est de la forme

- *$R_p=\pi_1\pi_2$ avec π_i irréductibles non associés de $\mathbb{Z}/p\mathbb{Z}[X]$, le nombre premier p est associé au produit de deux irréductibles non associés z_1 et z_2 dans A.*
- *$R_p=\pi^2$, avec π irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors p est associé au carré d'un irréductible z de A.*
- *$R_p=\pi$, avec π irréduction sur $\mathbb{Z}/p\mathbb{Z}[X]$, le nombre premier p est irréductible sur A.*

Ces résultats se généralisent de la façon suivante (à l'aide de la théorie des anneaux de Dedekind) : soient $P\in\mathbb{Z}[X]$ unitaire, α une racine complexe de P et A, l'anneau définit par

$$A=\mathbb{Z}[\alpha]=\{Q(\alpha),\quad Q\in\mathbb{Z}[X]\}$$

(dans notre cas $P=X^2-X+2$, $\alpha=\dfrac{1+i\sqrt{7}}{2}$ et $A=A$). Soit p un nombre premier, alors, sous certaines hypothèses (satisfaitent dans notre cas), si la réduction de P modulo p est de la forme $P=(\pi_1)^{e_1}\cdots(\pi_r)^{e_r}$ alors p se décompose dans A sous la forme $p=\varepsilon(z_1)^{e_1}\cdots(z_r)^{e_r}$, où les z_i sont des irréductibles de A (que l'on peut en fait construire explicitement à partir de p et de π_i) et ε un inversible de A.

Correction de l'exercice 1.3 : Comment par un petit rappel : l'anneau $\mathbb{R}[X]$ est euclidien, ce qui implique tout polynôme de $\mathbb{R}[X]$ s'écrit comme le produit de polynômes irréductibles. D'autre part, les irréductibles de $\mathbb{R}[X]$ sont tous les

polynômes du premier degré et tous les polynômes du second degré sans racines sur $\mathbb{R}$, c'est-à-dire à discriminant strictement négatif. Ainsi, tout polynôme P de $\mathbb{R}[X]$ s'écrit

$$P(X)=\lambda\left(\prod_{i\in I}(X-r_i)^{\alpha_i}\right)\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right),$$

où I et J sont deux ensembles finis (éventuellement vide et dans ce cas le produit est égal à 1), λ, r_i, a_j, b_j sont des réels avec $a_j^2-4b_j<0$ (discriminant strictement négatif) et les α_i et β_j sont des entiers naturels non nuls.
Remarquons que dans l'écriture de P nous avons factorisé les coefficients dominants des facteurs linéaires et du second degré et nous les avons regroupé dans la constante λ (d'où le fait que tous les facteurs ont un coefficient dominant égal à 1)

1. (a) Soit f un tel polynôme.
Si f est un polynôme constant C, puisque f est positif, la constante C est réelle positive donc elle admet une racine carrée réelle et l'on peut écrire $(\sqrt{C})^2$ avec $\sqrt{C}\in\mathbb{R}$, ce qui démontre le résultat attendu.
Si f est un polynôme non constant alors f s'écrit sous la forme $f(X)=\lambda\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right)$, où J est un ensemble fini non vide. Chaque trinôme étant de signe constant (car ils n'ont pas de racines dans $\mathbb{R}$) et leur coefficient dominant respectif étant 1, on en déduit qu'ils sont tous positifs sur $\mathbb{R}$. Puisque f est positif, la constante réelle λ l'est également donc on peut l'écrire $(\sqrt{\lambda})^2$ où $\sqrt{\lambda}$ est un réel.
Montrer que tout trinôme $X^2+a_jX+b_j$ s'écrit sous la forme $P_i^2+Q_i^2$, où P_i, Q_i sont des polynômes de $\mathbb{R}[X]$.
Pour commencer le trinôme admet comme discriminant le réel $\Delta_j=a_j^2-4b_j<0$ donc $-\Delta_j$ est strictement positif, ce qui permet de l'écrire $\Delta_j=-\delta_j^2$ (avec $\delta_j=\sqrt{-\Delta_j}$ par exemple). Ensuite, on utilise la célèbre méthode "du début d'un carré"

$$\begin{aligned}X^2+a_jX+b_j &= \left(X+\frac{a_j}{2}\right)^2-\frac{a_j^2}{4}+b_j=\left(X+\frac{a_j}{2}\right)^2+\frac{4b_j-a_j^2}{4}=\left(X+\frac{a_j}{2}\right)^2-\frac{\Delta_j}{4}\\ &= \left(X+\frac{a_j}{2}\right)^2+\frac{\delta_j^2}{4}=\left(X+\frac{a_j}{2}\right)^2+\left(\frac{\delta_j}{2}\right)^2\end{aligned}$$

Nous venons donc de montrer que tout trinôme $X^2+a_jX+b_j$ avec $a_j^2-4b_j<0$ s'écrit sous la forme $P_i^2+Q_i^2$.
Montrons par récurrence que tout polynôme F qui s'écrit comme le produit de n trinômes de la forme $X^2+a_jX+b_j$, avec $a_j^2-4b_j<0$, est de la forme $F=P^2+Q^2$.
Pour $n=1$, nous venons de le faire, supposons que cela soit vrai pour n. Soit F un polynôme égal au produit de $n+1$ trinômes de la forme $X^2+a_jX+b_j$. On peut appliquer alors l'hypothèse de récurrence au polynôme $S=\prod_{j=1}^{n}(X^2+a_jX+b_j)$ donc $S=P^2+Q^2$. D'autre part, on peut écrire $X^2+a_{n+1}X+b_{n+1}=A^2+B^2$, donc on a

$$\begin{aligned}F &= \prod_{j=1}^{n+1}(X^2+a_jX+b_j)=S\times(X^2+a_{n+1}X+b_{n+1})=(P^2+Q^2)(A^2+B^2)=(P+iQ)(P-iQ)(A+iB)(A-iB)\\ &= [(P+iQ)(A+iB)]\,[(P-iQ)(A-iB)]=[(PA-QB)+i(QA+PB)][(PA-QB)-i(QA+PB)]\\ &= (PA-QB)^2+(QA+PB)^2,\end{aligned}$$

ce qui montre que F s'écrit bien comme la somme de deux carrés. L'hérédité est donc démontré et cela achève la récurrence.
Remarque : Dans $\mathbb{C}$, on $|a+ib|^2=a^2+b^2$ si a et b sont réels et le produit de deux modules carré est un module carré (celui du produit), ce que l'on peut écrire comme le produit de deux sommes de deux carrés est la somme de deux carrés. La preuve étant purement algébrique, nous n'avons eu qu'à la retranscrire dans $\mathbb{R}[X]$.
Revenons à notre polynôme f. Nous savons maintenant que le polynôme $\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}$, qui est le produit de $\sum_{j\in J}\beta_j$ trinômes de discriminant strictement négatif, s'écrit

$$\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}=A^2+B^2;$$

où A, B sont deux éléments de $\mathbb{R}[X]$ et que λ s'écrit $(\sqrt{\lambda})^2$, où $\sqrt{\lambda}\in\mathbb{R}$, on en déduit que f s'écrit

$$f=(\sqrt{\lambda})^2(A^2+B^2)=(\sqrt{\lambda}A)^2+(\sqrt{\lambda}B)^2,$$

où $\sqrt{\lambda}A$ et $\sqrt{\lambda}B$ sont deux éléments de $\mathbb{R}[X]$. Le résultat escompté est démontré.

(b) Si f est scindé sur $\mathbb{R}[X]$. Soit f est non constant sur $\mathbb{R}$ et comme il est scindé, la constante est nécessairement nul et $f = 0 = 0^2$, soit f est non constant sur $\mathbb{R}$. Il s'écrit alors $f = \lambda\left(\prod_{i\in I}(X-r_i)^{\alpha_i}\right)$, où les r_i sont des réels deux à deux distincts, α_i des entiers naturels non nuls et λ une constante réelle non nulle. Les nombres α_i étant tous entiers naturels non nuls, ils s'écrivent tous sous la forme $\alpha_i = 2\gamma_i + \delta_i$ avec $\delta_i \in \{0,1\}$ (δ_i n'est que le reste de la division euclidienne de α_i par 2). Nous pouvons alors écrire f sous la forme

$$f = \lambda\left(\prod_{i\in I}(X-r_i)^{2\gamma_i}\right)\prod_{i\in I}(X-r_i)^{\delta_i} = \lambda\left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2\prod_{i\in I}(X-r_i)^{\delta_i}$$

(en fait, on vient d'extraire tous les facteurs carrés du produit). Puisque les polynômes f et $\left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2$ sont positifs sur $\mathbb{R}$ et que λ est de signe fixe (sic), on en déduit que le polynôme $\prod_{i\in I}(X-r_i)^{\delta_i}$ est de signe constant sur $\mathbb{R}$. Montrons alors que tous les δ_i sont nuls. On procède par l'absurde en supposant qu'un au moins des δ_i soient non nuls. Alors dans le produit $\prod_{i\in I}(X-r_i)^{\delta_i}$, les facteurs correspondant à $\delta_i = 0$ sont égaux à 1 et les facteurs correspondant à $\delta_i = 1$ sont de la forme $X - r_i$, ce qui permet d'écrire

$$\prod_{i\in I}(X-r_i)^{\delta_i} = (X-r_{i_1})\cdots(X-r_{i_q}),$$

où les r_{i_k} sont deux à deux distincts. Un tableau de signe nous montre alors clairement que

$$(X-r_{i_1})\cdots(X-r_{i_q}) = \prod_{i\in I}(X-r_i)^{\delta_i}$$

n'est pas signe constant donc tous les δ_i sont nuls, ce qui implique que f s'écrit

$$f = \lambda\left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2$$

Les polynômes f et $\left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2$ sont positifs sur $\mathbb{R}$ donc λ est positif et λ admet une racine carrée réelle. On peut dès lors écrire

$$f(X) = \sqrt{\lambda}^2\left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2 = \left(\sqrt{\lambda}\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2,$$

ce qui démontre le résultat attendu.

(c) Si f est un polynôme constant, cette constante λ est nécessairement positive donc elle admet une racine carré réelle et $f = (\sqrt{\lambda})^2$, ce qui démontre le résultat.
Si f est un polynôme non constant alors il s'écrit

$$f(X) = \lambda\left(\prod_{i\in I}(X-r_i)^{\alpha_i}\right)\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right) \text{ avec } \forall j\in J;\quad a_j^2-4b_j<0$$

Chaque trinôme $X^2 + a_jX + b_j$ étant positif sur $\mathbb{R}$ (sans racine sur $\mathbb{R}$ donc de signe constant et le coefficient dominant est 1), on en déduit que le produit $\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}$ est positif sur $\mathbb{R}$. Puisque les polynômes f et $\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}$ ainsi que la constante λ sont de signe constant sur $\mathbb{R}$, on en déduit que le produit $\prod_{i\in I}(X-r_i)^{\alpha_i}$ est de signe constant sur $\mathbb{R}$. Or nous avons vu dans la question 1.b) que le fait qu'un tel produit soit de signe constant implique que tous les exposants α_i sont pairs, donc ils s'écrivent $\alpha_i = 2\gamma_i$. On en déduit que f s'écrit

$$\underbrace{f(X)}_{\geqslant 0 \text{ sur } \mathbb{R}} = \lambda\left(\prod_{i\in I}(X-r_i)^{2\gamma_i}\right)\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right) = \underbrace{\lambda\left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2}_{\geqslant 0 \text{ sur } \mathbb{R}}\underbrace{\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}}_{\geqslant 0 \text{ sur } \mathbb{R}}$$

Cette dernière écriture implique clairement que λ est nécessairement positif donc il admet une racine carrée réelle, ce qui autorise l'égalité $\lambda = (\sqrt{\lambda})^2$ dans $\mathbb{R}$. La question 1.a) montre que le produit $\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}$ s'écrit A^2+B^2, où A, B sont deux polynômes réels. Si l'on note $C = \prod_{i\in I}(X-r_i)^{\gamma_i}$, nous avons l'égalité suivante

$$f(X) = (\sqrt{\lambda})^2C^2(A^2+B^2) = (\underbrace{\sqrt{\lambda}CA}_{\in\mathbb{R}[X]})^2 + (\underbrace{\sqrt{\lambda}CB}_{\in\mathbb{R}[X]})^2$$

qui démontre que f est bien la somme de deux carrés de polynômes réels.

2. Montrons qu'un tel polynôme s'écrit sous la forme

$$f(X) = E^2+F^2+X(G^2+K^2)$$

Si f est un polynôme constant, cette constante λ est nécessairement positive donc elle admet une racine carré réelle et $f = (\sqrt{\lambda})^2$, ce qui démontre le résultat annoncé ($E = \sqrt{\lambda}$, $F = G = K = 0$)
Si f est un polynôme non constant alors il s'écrit

$$f(X) = \lambda\left(\prod_{i\in I}(X-r_i)^{\alpha_i}\right)\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right) \text{ avec } \forall j\in J;\quad a_j^2-4b_j<0$$

Le produit $\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}$ étant positif sur $\mathbb{R}$ (donc sur $\mathbb{R}_+$), le polynôme f étant positif sur $\mathbb{R}_+$ et la constante λ étant de signe constant (!), on en déduit que le produit $\prod_{i\in I}(X-r_i)^{\alpha_i}$ est de signe constant sur $\mathbb{R}_+$.

- Si l'ensemble I est vide alors $\prod_{i\in I}(X-r_i)^{\alpha_i} = 1$ et l'on a

$$f(X) = \lambda\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right)$$

Les polynômes f et $\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right)$ étant positifs sur $\mathbb{R}_+$, on en déduit que λ est positive. Dans la question 1.a), on a vu que le produit $\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}$ peut s'écrire comme la somme de deux carrés, ce montre que le polynôme f s'écrit sous la forme E^2+F^2. Le résultat annoncé est prouvé ($G = K = 0$)

- Si l'ensemble I est non vide, comme dans la question 1.b), on peut écrire

$$\prod_{i\in I}(X-r_i)^{\alpha_i} = \left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2\prod_{i\in I}(X-r_i)^{\delta_i},$$

où $\forall i\in I,\quad r_i = 2\gamma_i+\delta_i$ et $\delta_i\in\{0,1\}$.
Si tous les δ_i sont nuls, alors

$$f = \lambda\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right)\prod_{i\in I}(X-r_i)^{\alpha_i} = \lambda\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right)\left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2$$

Puisque f, $\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right)$ et $\left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)$ sont positifs sur $\mathbb{R}_+$, on en déduit que λ est positf. Par conséquent, f est clairement positif sur $\mathbb{R}$ tout entier donc il s'écrit sous la forme E^2+F^2 et le résultat annoncé est prouvé ($G = K = 0$).
Si au moins de δ_i n'est pas nul, le produit $\prod_{i\in I}(X-r_i)^{\delta_i}$ peut alors s'écrire

$$\prod_{i\in I}(X-r_i)^{\delta_i} = (X-r_{i_1})\cdots(X-r_{i_q})$$

(les facteurs correspondant aux cas $\delta_i = 0$ étant égaux à 1). Il est évident que si r_{i_k} est négatif alors $X-r_{i_k}$ est positif sur $\mathbb{R}_+$ (somme de deux positifs).
Supposons qu'au moins une racine est strictement positive. Le produit $(X-r_{i_1})\cdots(X-r_{i_q})$ peut s'écrire

$$(X-r_{i_1})\cdots(X-r_{i_q}) = \left[(X-r_{n_1})\cdots(X-r_{n_s})\right]\left[(X-r_{m_1})\cdots(X-r_{m_t})\right],$$

où les r_{n_k} sont les racines négatives et les r_{m_k} sont strictement positives. Le produit $(X-r_{n_1})\cdots(X-r_{n_s})$ est alors positif sur $\mathbb{R}_+$ (addition de deux positifs est positif puis produit de positifs) alors que le produit $(X-r_{m_1})\cdots(X-r_{m_t})$ n'est pas de signe constant sur $\mathbb{R}_+$ (il suffit de dresser le tableau de signe de ce produit en distinguant le cas $t=1$ du cas $t\geqslant 2$). On en déduit que le produit

$$[(X-r_{n_1})\cdots(X-r_{n_s})]\left[(X-r_{m_1})\cdots(X-r_{m_t})\right]=(X-r_{i_1})\cdots(X-r_{i_q})=\prod_{i\in I}(X-r_i)^{\delta_i}$$

n'est pas de signe constant sur $\mathbb{R}_+$, ce qui est une contradiction flagrante.
Par conséquent, tous les racines r_{i_k} sont négatives, ce qui nous permet de les écrire $r_{i_k}=-s_{i_k}^2$, où les s_{i_k} des réels. On en déduit que f s'écrit

$$\underbrace{f(X)}_{\geqslant 0 \text{ sur } \mathbb{R}_+}=\lambda\left(\underbrace{\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}}_{\geqslant 0 \text{ sur } \mathbb{R}_+}\right)\underbrace{\left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2}_{\geqslant 0 \text{ sur } \mathbb{R}_+}(\underbrace{X+s_{i_1}^2}_{\geqslant 0 \text{ sur } \mathbb{R}_+})\cdots(\underbrace{X+s_{i_q}^2}_{\geqslant 0 \text{ sur } \mathbb{R}_+})$$

ce qui implique λ est positif. Si l'on considère le polynôme Q défini par

$$Q(X)=\lambda\left(\prod_{j\in J}(X^2+a_jX+b_j)^{\beta_j}\right)\left(\prod_{i\in I}(X-r_i)^{\gamma_i}\right)^2,$$

on constate aisément que Q est positif sur $\mathbb{R}$ tout entier, donc il s'écrit sous la forme A^2+B^2. On en déduit alors que

$$Q(X)(X+s_{i_1}^2)=(A^2+B^2)(X+s_{i_1}^2)=(s_{i_1}A)^2+(s_{i_1}B^2)+X(A^2+B^2),$$

ce qui signifie que le polynôme s'écrit sous la forme

$$Q(X)(X+s_{i_1}^2)=C^2+D^2+X(A^2+B^2)$$

Ensuite, on a

$$\begin{aligned}Q(X)(X+s_{i_1}^2)(X+s_{i_2}^2) &= (C^2+D^2+X(A^2+B^2))(X+s_{i_2}^2)\\ &= (s_{i_1}C)^2+(s_{i_2}D)^2+(XA)^2+(XB)^2+X[(s_{i_2}A)^2+(s_{i_2}B)^2+C^2+D^2]\end{aligned}$$

Il est évident que les polynômes $(s_{i_1}C)^2+(s_{i_2}D)^2+(XA)^2+(XB)^2$ et $(s_{i_2}A)^2+(s_{i_2}B)^2+C^2+D^2$ sont positifs sur $\mathbb{R}$ tout entier donc ils s'écrivent chacun comme la somme de deux carrés. Nous avons alors l'égalité suivante

$$Q(X)(X+s_{i_1}^2)(X+s_{i_2}^2)=(C_1)^2+(D_1)^2+X((A_1)^2+(B_1)^2)$$

En procédant par itération, on en déduit que le produit $Q(X)(X+s_{i_1}^2)\cdots(X+s_{i_q}^2)$ s'écrit sous la forme $E^2+F^2+X(G^2+K^2)$, où E,F,G,K sont des polynômes de $\mathbb{R}[X]$ et le résultat annoncé est encore démontré.